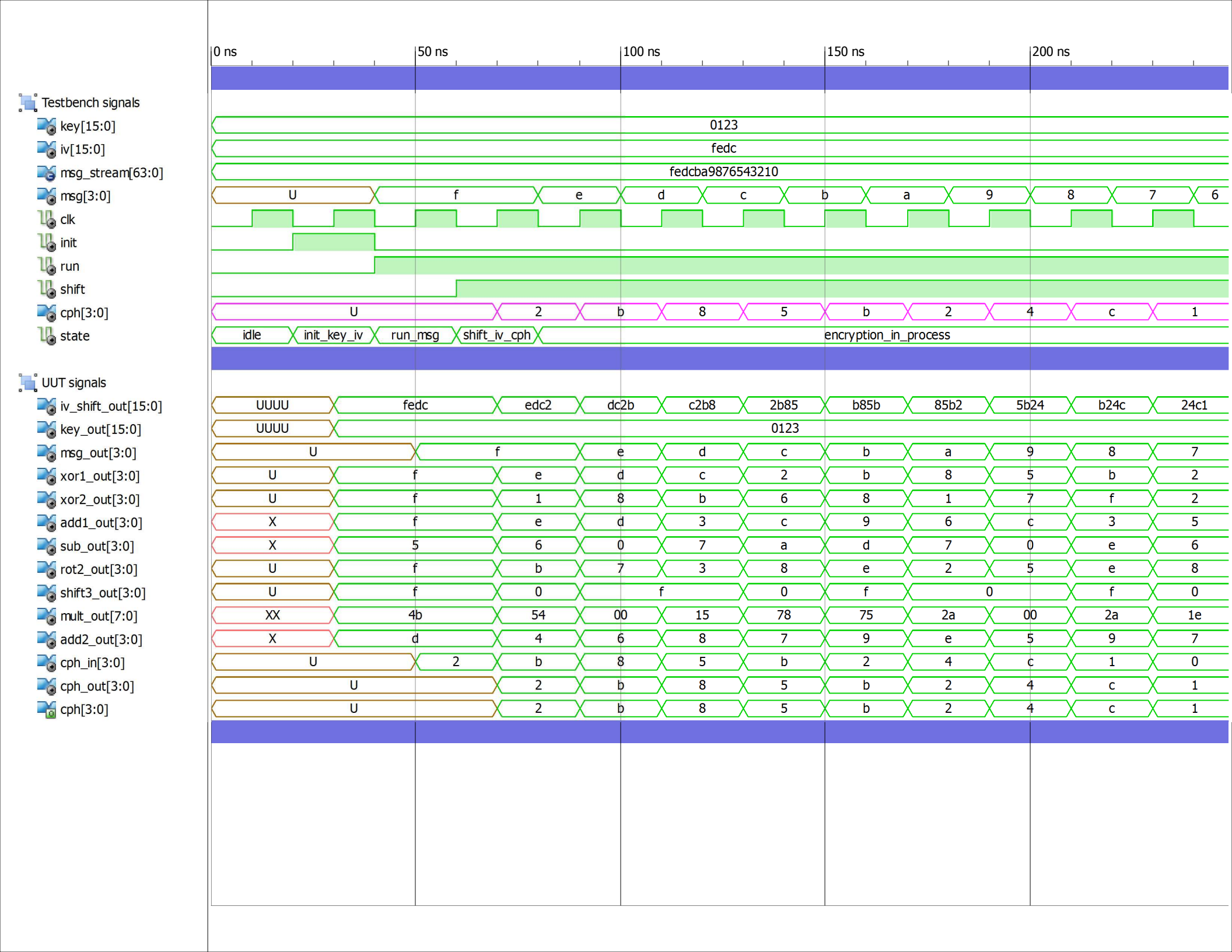
0 ns
50 ns
100 ns
150 ns
200 ns
Testbench signals
key[15:0]
iv[15:0]
msg_stream[63:0]
msg[3:0]
clk
init
run
shift
cph[3:0]
state
0123
fedc
fedcba9876543210
U f e d c b a 9 8 7 6
U 2 b 8 5 b 2 4 c 1
idle
init_key_iv
run_msg
shift_iv_cph
encryption_in_process
UUT signals
iv_shift_out[15:0]
key_out[15:0]
msg_out[3:0]
xor1_out[3:0]
xor2_out[3:0]
add1_out[3:0]
sub_out[3:0]
rot2_out[3:0]
shift3_out[3:0]
mult_out[7:0]
add2_out[3:0]
cph_in[3:0]
cph_out[3:0]
cph[3:0]
UUUU fedc edc2 dc2b c2b8 2b85 b85b 85b2 5b24 b24c 24c1
UUUU 0123
U f e d c b a 9 8 7
U f e d c 2 b 8 5 b 2
U f 1 8 b 6 8 1 7 f 2
X f e d 3 c 9 6 c 3 5
X 5 6 0 7 a d 7 0 e 6
U f b 7 3 8 e 2 5 e 8
U f 0 f 0 f 0 f 0
XX 4b 54 00 15 78 75 2a 00 2a 1e
X d 4 6 8 7 9 e 5 9 7
U 2 b 8 5 b 2 4 c 1 0
U 2 b 8 5 b 2 4 c 1
U 2 b 8 5 b 2 4 c 1


360.335 ns
300 ns
350 ns
400 ns
450 ns
Testbench signals
key[15:0]
iv[15:0]
msg_stream[63:0]
msg[3:0]
clk
init
run
shift
cph[3:0]
state
0123
fedc
fedcba9876543210
6 5 4 3 2 1 0
0 8 3 a d 1 7 8
encryption_in_process
stop_msg
stop_shift
UUT signals
iv_shift_out[15:0]
key_out[15:0]
msg_out[3:0]
xor1_out[3:0]
xor2_out[3:0]
add1_out[3:0]
sub_out[3:0]
rot2_out[3:0]
shift3_out[3:0]
mult_out[7:0]
add2_out[3:0]
cph_in[3:0]
cph_out[3:0]
cph[3:0]
4c10 c108 1083 083a 83ad 3ad1 ad17 d178
0123
6 5 4 3 2 1 0
4 c 1 0 8 3 a d
3 b 0 9 e 2 4 b
d 2 1 9 4 b e 2
1 2 a f 8 5 1 b
1 3 4 0 2 c a 7
0 f 0 f 0 f
0d 04 0a 87 20 37 0e 16
e 6 e 3 6 8 d
8 3 a d 1 7 8 d
0 8 3 a d 1 7 8
0 8 3 a d 1 7 8